20

30

Claims

- 1. A method of authenticating a client to a communication system comprising the steps of
- receiving from a mobile station a subscriber identity corresponding to a subscriber of a mobile telecommunication network, wherein the mobile telecommunication network is separate from the communication system to which the client is to be authenticated;

sending the subscriber identity to an authentication block of the mobile telecommunication network;

receiving from the authentication block at least one challenge and at least one first secret based on a subscriber's secret specific to the subscriber identity;

sending the at least one challenge to the subscriber identity module;

receiving at least one second secret in response to the at least one challenge; and using the second secret for authenticating the client.

 The method of authenticating of claim 1 further comprising: receiving a PIN from a user; and transmitting wirelessly the PIN to the mobile station.

3. The method according to claim 2 further comprising:

encrypting the PIN before the step of transmitting.

- The method according to claim 1 wherein the step of using further comprises:
 encrypting the second secret to provide a encrypted second secret; and
 transmitting the encrypted second secret to the communication system.
 - 5. The method according to claim 4 wherein the step of using further comprises: refreshing the encrypted second secret.
 - 6. The method according to claim 1 wherein the step of sending the subscriber

14

identity to an authentication block comprises sending wirelessly the subscriber identity to the authentication block; and the step of receiving from the authentication block comprises receiving wirelessly from the authentication block.

5

10

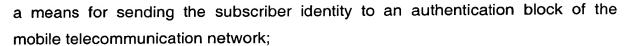
15

25

30

- 7. The method according to claim 1 wherein the steps of receiving from a mobile station a subscriber identity comprises receiving wirelessly from a mobile station a subscriber identity; sending the at least one challenge comprises sending wirelessly the at least one challenge; and receiving at least one second secret comprises receiving wirelessly at least one second secret.
- 8. The method of authenticating of claim 7 further comprising: receiving a PIN from a user; and transmitting wirelessly the PIN to the mobile station.
- 9. The method of authenticating of claim 8 wherein the step of transmitting wirelessly comprises transmitting an infrared signal.
- 20 10. The method of authenticating of claim 8 wherein the step of transmitting wirelessly comprises transmitting a radio signal.
 - 11. The method of authenticating of claim 8 wherein the step of transmitting wirelessly comprises transmitting a low power radio signal.
 - 12. The method of authenticating of claim 8 wherein the step of transmitting wirelessly comprises transmitting an acoustic signal.
 - 13. A client for authenticating a client to a communication system comprising: a means for receiving from a mobile station a subscriber identity corresponding to a subscriber of a mobile telecommunication network, wherein the mobile telecommunication network is separate from the communication system to which the client is to be authenticated;

5



a means for receiving from the authentication block at least one challenge and at least one first secret based on a subscriber's secret specific to the subscriber identity;

a means for sending the at least one challenge to the subscriber identity module; a means for receiving at least one second secret in response to the at least one challenge; and

a means for using the second secret for authenticating the client.

10 14. The client for authenticating of claim 13 further comprising:

a means for receiving a PIN from a user; and

a means for transmitting wirelessly the PIN to the mobile station.

15. The client according to claim 14 further comprising:

a means for encrypting the PIN before the step of transmitting.

15 16. The client according to claim 13 wherein means for using further comprises:

a means for encrypting the second secret to provide a encrypted second secret; and

a means for transmitting the encrypted second secret to the communication system.

- 20 17. The method according to claim 16 wherein the step of using further comprises: refreshing the encrypted second secret.
 - 18. The client according to claim 13 wherein the a means for sending the subscriber identity to an authentication block comprises a means for sending wirelessly the subscriber identity to the authentication block; and the a means for receiving from the authentication block comprises a means for receiving wirelessly from the authentication block.
 - 19. The client according to claim 13 wherein
 - a means for receiving from a mobile station a subscriber identity comprises a means for receiving wirelessly from a mobile station a subscriber identity;
- a means for sending the at least one challenge comprises a means for sending wirelessly the at least one challenge; and

30

5

a means for receiving at least one second secret comprises a means for receiving wirelessly at least one second secret

- 20. The client of claim 19 further comprising:
 - a means for receiving a PIN from a user; and
 - a means for transmitting wirelessly the PIN to the mobile station.
- 21. The client of claim 19 wherein the a means for transmitting wirelessly comprises a means for transmitting an infrared signal.
- 22. The client of claim 19 wherein the a means for transmitting wirelessly comprises a means for transmitting a radio signal.
- 10 23. The client of claim 19 wherein the a means for transmitting wirelessly comprises a means for transmitting a low power radio signal.
 - 24. The client of claim 19 wherein the a means for transmitting wirelessly comprises a means for transmitting an acoustic signal.
- 15 25.A method for providing at least one secret based on a subscriber identity comprising the steps of:
 - retrieving from a subscriber identity module a subscriber identity corresponding to a subscriber of a mobile telecommunication network;
 - sending wirelessly the subscriber identity to a client for authenticating the client to the communication system;
 - receiving wirelessly from the client at least one challenge based on a subscriber's secret specific to the subscriber identity;
 - generating at least one secret in response to the at least one challenge and sending wirelessly the at least one secret.
- 25 26. The method of claim 25 wherein the method further comprises a step of wirelessly receiving a request.
 - 27. The method of claim 26 wherein the request contains a PIN.
 - 28. The method of claim 27 wherein the request contains an encrypted PIN.
 - 29. The method of claim 27 further comprising a step of confirming that the PIN matches a identity module PIN.
 - 30. A mobile station for providing at least one secret based on a subscriber identity

comprising:

means for retreiving from a subscriber identity module a subscriber identity corresponding to a subscriber of a mobile telecommunication network;

means for sending wirelessly the subscriber identity to a client for authenticating the client to the communication system;

means for receiving wirelessly from the client at least one challenge based on a subscriber's secret specific to the subscriber identity;

means for generating at least one secret in response to the at least one challenge and

- means for sending wirelessly the at least one secret.
 - 31. The mobile station of claim 30 wherein the method further comprises a means for wirelessly receiving a request.
 - 32. The mobile station of claim 31 wherein the request contains a PIN.
 - 33. The mobile station of claim 32 wherein the request contains an encrypted PIN.
- 15 34. The mobile station of claim 32 further comprising means for confirming that the PIN matches a identity module PIN.